AA 01: Safety and Security Assurance

Application Area Summary

Purpose

The purpose of Safety and Security Assurance is to establish and maintain a safety and security capability, define and manage requirements based on risks attributable to threats, hazards, and vulnerabilities, and assure that products and services are safe and secure.

Goals

1. **An infrastructure for safety and security is established and maintained.**
   (AP 01.01, AP 01.02, AP 01.03, AP 01.04 AP 01.05)
2. **Safety and security risks are identified and managed.**
   (AP 01.06, AP 01.07, AP 01.08)
3. **Safety and security requirements are satisfied.**
   (AP 01.09, AP 01.10, AP 01.11, AP 01.12)
4. **Activities and products are managed to achieve safety and security requirements and objectives.**
   (AP 01.13, AP 01.14, AP 01.15, AP 01.16)

Application Practice List

AP 01.01 **Ensure Safety and Security Competency**
Ensure safety and security awareness, guidance and competency.

AP 01.02 **Establish Qualified Work Environment**
Establish and maintain a qualified work environment that meets safety and security needs.

AP 01.03 **Control Information**
Establish and maintain storage, protection and access and distribution control to assure the integrity of information.

AP 01.04 **Monitor Incidents**
Monitor, report and analyze safety and security incidents and identify potential corrective actions.

AP 01.05 **Ensure Business Continuity**
Plan and provide for continuity of activities with contingencies for threats and hazards to operations and the infrastructure.

AP 01.06 **Identify Safety and Security Risks**
Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.

AP 01.07 **Analyze and Prioritize Risks**
For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence and determine relative priority.

AP 01.08 **Determine, Implement and Monitor Risk Mitigation Plan**
For each risk associated with safety or security, determine, implement and monitor the risk mitigation plan to achieve an acceptable level of risk.

AP 01.09 **Identify Regulatory Requirements, Laws and Standards**
Identify and document applicable regulatory requirements, laws, standards, policies, and acceptable levels of safety and security**.**

AP 01.10 **Establish Safety and Security Requirements and Design**
Establish and maintain safety and security requirements, including integrity levels, and design the product or service to meet them.

AP 01.11 **Objectively Evaluate Products**
Objectively verify and validate the work products and delivered products and services to assure safety and security requirements have been achieved and services fulfill intended use.

AP 01.12 **Establish Safety and Security Assurance Argument**
Establish and maintain safety and security assurance arguments and supporting evidence throughout the lifecycle.

AP 01.13 **Establish Independent Safety and Security Reporting**
Establish and maintain independent reporting of safety and security status and issues.

AP 01.14 **Establish a Safety and Security Assurance Plan**
Establish and maintain a plan to achieve safety and security assurance requirements and objectives.

AP 01.15 **Select and Manage Suppliers, Products and Services**
Select and manage products and suppliers using safety and security criteria.

AP 01.16 **Monitor and Control Activities and Products**
Measure, monitor and review safety and security activities against plans, control products, take corrective action, and improve processes.

Relationships between this Application Area and the Reference Models
This Application Area is to be used in conjunction with the Capability Maturity Model Integration (CMMI) or the FAA integrated Capability Maturity Model (iCMM).

Process Areas: This Application Area draws on implementing practices from the following PAs for use with either the iCMM or CMMI. Where indicated, material from the iCMM PAs would be adopted for use in the CMMI. The particular implementing practices from these PAs are provided along with the discussion of each application practice (AP).

iCMM PAs	CMMI PAs *(including extensions from iCMM)*
PA 22 Training	Organizational Training
PA 19 Work Environment*	Work Environment*
PA 17 Information Management	*PA 17 Information Management (from iCMM)*
PA 10 Operation and Support	*PA 10 Operation and Support (from iCMM)*
PA 13 Risk Management	Risk Management
PA 00 Integrated Enterprise Management	*PA 00 Integrated Enterprise Management (from iCMM)* Organizational Environment for Integration Organizational Innovation and Deployment
PA 01 Needs PA 02 Requirements	Requirements Development Requirements Management
PA 03 Design	Technical Solution
PA 08 Evaluation	Verification Validation

iCMM PAs	CMMI PAs *(including extensions from iCMM)*
PA 15 Quality Assurance & Management	Process and Product Quality Assurance
PA 11 Project Management	Project Planning Project Monitoring and Control Integrated Project Management Quantitative Project Management
PA 16 Configuration Management	Configuration Management
PA 18 Measurement and Analysis	Measurement and Analysis
PA 05 Outsourcing PA 12 Supplier Agreement Management PA 09 Deployment, Transition, & Disposal	Supplier Agreement Management Integrated Supplier Management
PA 21 Process Improvement	Organizational Process Focus

* Work Environment is a new Process Area for CMMI and iCMM (see description in review package)

Generic Practices: As with Process Areas in the CMMI and the iCMM, generic practices are applied to the Application Area to guide process improvement and to support appraisal of capabilities. The generic practices of iCMM and CMMI are depicted below:

	iCMM Generic Practices	CMMI Generic Practices
Capability Level 1	1.1 Identify the Work Scope 1.2 Perform the Process	1.1 Perform Base Practices
Capability Level 2	2.1 Establish Organizational Policy 2.2 Document the Process 2.3 Plan the Process 2.4 Provide Adequate Resources 2.5 Assign Responsibility 2.6 Ensure Skill and Knowledge 2.7 Establish Work Product Requirements 2.8 Consistently Use and Manage the Process 2.9 Manage Work Products 2.10 Objectively Assess Process Compliance 2.11 Objectively Verify Work Products 2.12 Measure Process Performance 2.13 Review Performance with Higher-level Mgmt 2.14 Take Corrective Action 2.15 Coordinate With Participants & Stakeholders	2.1 Establish an Organizational Policy 2.2 Plan the Process 2.3 Provide Resources 2.4 Assign Responsibility 2.5 Train People 2.6 Manage Configurations 2.7 Identify and Involve Relevant Stakeholders 2.8 Monitor and Control the Process 2.9 Objectively Evaluate Adherence 2.10 Review Status with Higher Level Management
Capability Level 3	3.1 Standardize the Process 3.2 Establish and Use a Defined Process 3.3 Improve Processes	3.1 Establish a Defined Process 3.2 Collect Improvement Information
Capability Level 4	4.1 Stabilize Process Performance	4.1 Establish Quantitative Objectives for Process 4.2 Stabilize Subprocess Performance
Capability Level 5	5.1 Pursue Process Optimization	5.1 Ensure Continuous Process Improvement 5.2 Correct Root Causes of Problems

Glossary

A glossary is attached as an appendix to this Application Area.

AP 01.01 Ensure Safety and Security Competency

Ensure safety and security awareness, guidance and competency.

Description
For safety:
All persons involved in any safety lifecycle activity, including management activities, should have the appropriate training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform. The training, experience and qualifications of all persons involved in safety lifecycle activities, including any management of functional safety activities, should be assessed in relation to the particular application.

For security:
The information security manager, or individuals given the responsibility of security should work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs. The information security manager, or individuals given the responsibility of security should provide security related guidance to the organization. Manage security awareness, training, and education programs for all users and administrators. Identify needed improvements in skill and knowledge throughout the organization using the projects' needs, organizational strategic plan, and existing employee skills as guidance. Train personnel to have the skills and knowledge needed to perform their assigned roles. Assess the effectiveness of the training to meet the identified training needs. Provide security related guidance to the other engineering groups. Security engineering guidance is used by the engineering groups to make decisions about architecture, design, and implementation choice. Provide security related guidance to operational system users and administrators- this guidance tells the users and administrators what must be done to install, configure, operate, and decommission the system in a secure manner.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 22 Training BP 22.01 Identify training needs for the organization, projects, teams, and support groups. BP 22.02 Establish and maintain a training plan. BP 22.03 Establish and maintain training capability and delivery mechanisms to address identified training needs. BP 22.04 Train individuals to have the skills and knowledge needed to perform their assigned roles. BP 22.05 Establish and maintain records of training and experience. BP 22.06 Assess the effectiveness of training to meet identified training needs. BP 22.07 Establish and maintain an environment that encourages learning.	*Organizational Training (OT)* OT SP 1.1-1 Establish and maintain the strategic training needs of the organization. OT SP 1.2-1 Determine which training needs are the responsibility of the organization and which will be left to the individual project or support group. OT SP 1.3-1 Establish and maintain an organizational training tactical plan. OT SP 1.4-1 Establish and maintain training capability to address organizational training needs. OT SP 2.1-1 Deliver the training following the organizational training tactical plan. OT SP 2.2-1 Establish and maintain records of the organizational training. OT SP 2.3-1 Assess the effectiveness of the organization's training program.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 19 Work Environment BP 19.05 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.	*Work Environment (WE)* WE SP 1.5 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.

Typical Work Products

- Human Capital Plan
- Training plans
- Safety or security certifications
- Skills assessment
- Competency assessment

Notes

For Safety:

The following factors should be considered when assessing the competence of persons to carry out their duties:

1. engineering knowledge appropriate to the application area;
2. engineering knowledge appropriate to the technology (for example electrical, electronic, programmable electronic, software engineering, accident investigation, human factors);
3. safety engineering knowledge appropriate to the technology;
4. knowledge of the legal and safety regulatory framework;
5. the consequences in the event of failure of safety-related systems – the greater the consequences the more rigorous should be the specification and assessment of competence;
6. the safety integrity levels of safety-related systems – the higher the safety integrity levels the more rigorous should be the specification and assessment of competence;
7. the novelty of the design, design procedures or application – the newer or more untried the designs, design procedures or application, the more rigorous the specification and assessment of competence should be;
8. previous experience and its relevance to the specific duties to be performed and the technology being employed – the greater the required competence levels, the closer the fit should be between the competencies developed from previous experience and those required for the specific duties to be undertaken;
9. relevance of qualifications to specific duties to be performed.

The training, experience and qualifications of all persons involved in safety lifecycle activities should be documented.

AP 01.02 Establish Qualified Work Environment

Establish and maintain a qualified work environment that meets safety and security needs.

Description
Maintain the work environment to continuously support the projects that dependent on it. Identify new product technologies or enabling infrastructure that will help the organization acquire, develop, and apply technology for competitive advantage. Maintain awareness of the technologies that support the organization's goals. Insert new technologies into the work environment based on the organization's business goals and the project's needs.

For safety: The work environment is a critical component of the design, development, operation and maintenance of safety related systems. An appropriate work environment (including the set of integrated tools, techniques, measures and standards) needs to be selected, applied and qualified to satisfy the required safety integrity level over the whole safety lifecycle. The work environment should be included as part of any functional safety assessment of the system (refer AP 01.11). Consideration should be given to the availability of suitable tools over the entire lifecycle.

For security: Establish, maintain, and monitor written agreements with third parties who access an organization's assets (i.e., information, facilities, systems). Establish a management authorization process for new information processing facilities (such as hardware and software). Establish, operate, and maintain a security architecture comprising facilities, information systems, information technology and security personnel, security policy, physical security, and personnel security.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 19 Work Environment (NEW) BP 19.01 Establish and maintain the needs and requirements to implement, operate and sustain work environments. BP 19.02 Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements. BP 19.03 Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs. BP 19.04 Maintain the required qualification of work environment components. BP 19.05 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment. BP 19.06 Monitor, evaluate and insert, as appropriate, new technology for improving the work environment. BP 19.07 Plan and provide for continuity of the work	*Work Environment (WE) (NEW)* WE SP 1.1 Establish and maintain the needs and requirements to implement, operate and sustain work environments. WE SP 1.2 Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements. WE SP 1.3 Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs. WE SP 1.4 Maintain the required qualification of work environment components. WE SP 1.5 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment. WE SP 1.6 Monitor, evaluate and insert, as appropriate, new technology for improving the work environment. WE SP 1.7 Plan and provide for continuity of the work

iCMM Implementing Practices	*CMMI Implementing Practices*
environment.	environment.

Typical Work Products

- Safety Plans
- Work Environment Specification(s)

AP 01.03 Control Information

Establish and maintain storage, protection, and access and distribution control to assure the integrity of information.

Description
For safety: Identify and control safety information, data and safety assurance evidence. Ensure that artifacts related to safety assurance and evaluation are suitably protected.

For security: Identify and control security assurance evidence. Ensure that the artifacts related to security monitoring are suitably protected.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices (from iCMM)*
PA 17 Information Management BP 17.01 Establish and maintain a strategy and requirements for information management. BP 17.02 Establish an infrastructure for information management including repository, tools, equipment, and procedures. BP 17.03 Collect, receive, and store information according to established strategy and procedures. BP 17.04 Disseminate or provide timely access to information to those that need it. BP 17.05 Protect information from loss, damage, or unwarranted access. BP 17.06 Establish requirements and standards for content and format of selected information items.	*PA 17 Information Management (from iCMM)* BP 17.01 Establish and maintain a strategy and requirements for information management. BP 17.02 Establish an infrastructure for information management including repository, tools, equipment, and procedures. BP 17.03 Collect, receive, and store information according to established strategy and procedures. BP 17.04 Disseminate or provide timely access to information to those that need it. BP 17.05 Protect information from loss, damage, or unwarranted access. BP 17.06 Establish requirements and standards for content and format of selected information items.

Include requirements for safety and security assurance information when implementing BP 17.01 and BP 17.06.

Typical Work Products

- Hazard Log
- Safety Case
- Safety Argument
- Data Reporting Analysis and Corrective Action System (DRACAS)
- Repository

Notes
See AP 01.12 for descriptions of typical safety and security assurance information to be controlled.

For safety: Repository stores hazard records, safety argument and supporting evidence
Example hazard record information:

- A complete description of the hazard

- Who identified the hazard and when
- What are the consequences of the hazard and the severity of any resulting accidents
- What could cause the hazard
- Risk assessment of the hazard
- Causal Factors
- How the hazard will be detected, controlled or mitigated
- Safety requirements that are derived from the hazard
- Where the safety requirements are addressed in the design
- Verification requirements that are derived from the safety requirements
- Verification records
- Cross-references to other documents (that may document the above).

For security: Security assurance evidence repository (e.g., database, engineering notebook, test results, evidence log) stores all evidence generated during design, development, testing, and use. Could take the form of a database, engineering notebook, test results, or evidence log.

AP 01.04 Monitor Incidents

Monitor, report and analyze safety and security incidents and identify potential corrective actions.

Description
For safety: A closed loop system should be in place for reporting, collecting, recording, analyzing, investigating and initiating timely corrective actions on all incidents that may have an impact on safety.

For all proposed system changes, an impact analysis shall be carried out which shall include an assessment of the impact of the proposed modification or retrofit activity on the functional safety of the system. The assessment shall include a hazard and risk analysis sufficient to determine the breadth and depth to which subsequent overall safety lifecycle activities will need to be undertaken. The assessment shall also consider the impact of other concurrent modification or retrofit activities, and shall consider the functional safety both during and after the modification and retrofit activities have taken place. After modification, safety related systems shall be verified and revalidated.

Safety-related incidents that arise during the project lifecycle are reported. Incidents are resolved by reviewing against existing hazard analysis and risk assessment, updating the analysis as necessary. The resolution of such incidents may result in the need for updates to artifacts both inside and outside normal safety activities.

For security: Ensure all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security are identified and reported. Monitor changes in threats, vulnerabilities, impacts, risks, and the environment. Identify relevant security incidents. Monitor the performance and functional effectiveness of security safeguards. Review the security posture of the system to identify necessary changes. Examine historical and event records (compositions of log records) for security relevant information. Monitor ongoing changes in the risk spectrum and changes to their characteristics. Monitor ongoing changes in the impacts.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices (from iCMM)*
PA 10 Operation and Support BP 10.01 Operate the system, product, or service in its intended environment and in the specified way. BP 10.02 Monitor and evaluate capacity, service, and performance of the system, product, or service. BP 10.05 Perform failure identification actions when a non-compliance has occurred in the product or delivered service. BP 10.06 Take corrective action when appropriate (e.g., defective part, human error), or initiate	*PA 10 Operation and Support (from iCMM)* BP 10.01 Operate the system, product, or service in its intended environment and in the specified way. BP 10.02 Monitor and evaluate capacity, service, and performance of the system, product, or service. BP 10.05 Perform failure identification actions when a non-compliance has occurred in the product or delivered service. BP 10.06 Take corrective action when appropriate (e.g., defective part, human error), or initiate

iCMM Implementing Practices	*CMMI Implementing Practices (from iCMM)*
corrective action for product or service modification. BP 10.07 Establish a service to answer customer and user questions and help resolve problems they encounter.	corrective action for product or service modification. BP 10.07 Establish a service to answer customer and user questions and help resolve problems they encounter.

Ensure that safety and security incidents are included when implementing BP 10.02, and that failure analysis is performed when implementing BP 10.05.

Typical Work Products

- Minutes of meetings (e.g., of the safety management group)
- Updated project safety plan
- Updated threat analyses
- Updated Safety Case
- Updated threat Log
- Incident reports
- Change requests
- Engineering Change Proposals (with safety analysis)

AP 01.05 Ensure Business Continuity

Plan and provide for continuity of activities with contingencies for threats and hazards to operations and the infrastructure.

Description
To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters:

- There should be a managed process in place for developing and maintaining business continuity throughout the organization.
- Plans should be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes.
- A single framework of business continuity plans should be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.
- Business continuity plans should be tested regularly to ensure that they are up to date and effective.
- Business continuity plans should be maintained by regular reviews and updates to ensure their continuing effectiveness.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 19 Work Environment BP 19.07 Plan and provide for continuity of the work environment.	*Work Environment (WE)* WE SP 1.7 Plan and provide for continuity of the work environment.
PA 13 Risk Management BP 13.01 Establish and maintain an approach for managing risk that is the basis for identifying, assessing, mitigating, and monitoring risks for the life of the project. BP 13.02 Identify project risks by examining objectives, alternatives, and constraints in the context of established sources of risk. BP 13.03 Assess risks to determine their likelihood of occurrence and the consequences if they occur. BP 13.04 Develop risk mitigation plans for risks that meet risk action criteria defined by the risk management approach. BP 13.05 Implement, monitor, and control risk mitigation activities in accordance with risk mitigation plans.	*Risk Management (RSKM)* RSKM SP 1.1-1 Determine risk sources and categories. RSKM SP 1.2-1 Define the parameters used to analyze and categorize risks, and the parameters used to control the risk management effort. RSKM SP 1.3-1 Establish and maintain the strategy to be used for risk management. RSKM SP 2.1-1 Identify and document the risks. RSKM SP 2.2-1 Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority. RSKM SP 3.1-1 Develop a risk mitigation plan for the most important risks to the project, as defined by the risk management strategy. RSKM SP 3.2-1 Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.
PA 00 Integrated Enterprise Management BP 00.03 Establish and maintain the enterprise strategic plans that identify business objectives to be achieved, areas of business to be pursued and their interrelationships, and the significant goals to be	*PA 00 Integrated Enterprise Management (from iCMM)* BP 00.03 Establish and maintain the enterprise

iCMM Implementing Practices	*CMMI Implementing Practices*
accomplished.	strategic plans that identify business objectives to be achieved, areas of business to be pursued and their interrelationships, and the significant goals to be accomplished.

Typical work Products

- Business Continuity Plan
- Business Impact Analysis
- Information Technology Contingency Plan
- Business Contingency Plan
- Test Plan
- Training Exercises

Notes

For safety:

Business Continuity plans should be developed for programs that accept high safety risk in order to plan and execute an effective recovery process.

AP 01.06 Identify Safety and Security Risks

Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.

Description
For safety: The identification of potential accidents is a useful first step in the hazard identification process. Identifying sources of hazards helps to provide a structure to the hazard identification, and helps ensure completeness. The types of hazard sources, or accident-initiating events, that should be considered include component failures, procedural faults, human error and energy sources (explosive, electrical etc). The review of safety experiences on similar systems including mishap/incident hazard tracking logs (if accessible), lessons-learned, checklists, history, etc, provides a good foundation for the hazard identification process. Hazard identification shall be initiated at the earliest possible stage of the project lifecycle and should be based on an appropriate model of the system. It is important that the hazard identification is as complete as possible. The earlier hazards are identified the easier and more cost-effective it will be to deal with them

For security: Identify applicable threats arising from a natural source, and from man-made sources either accidental or deliberate. Identify system vulnerabilities. Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system. Identify and characterize the system assets that support the key capabilities or the security objectives of the system. Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics. Monitor ongoing changes in the threat spectrum and changes to their characteristics.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 13 Risk Management BP 13.02 Identify project risks by examining objectives, alternatives, and constraints in the context of established sources of risk.	*Risk Management (RSKM)* RSKM SP 2.1-1 Identify and document the risks.

Typical Work Products
- Accident list
- Hazard source lists (external and internal)
- Hazard log
- Hazard category lists
- System Environment and Boundary Definition
- Hazard Analysis Scope Definition
- System Functional Model
- Hazard and Operability Analysis
- Functional Failure Analysis (FFA) tables

- Preliminary Hazard List

Notes
For safety: Different standards use different terminology to describe accidents. Other terminology used includes "mishaps" and "hazardous events".
The following are examples of a potential accident.

- In an aircraft a potential accident is mid-air collision.
- In a process plant a potential accident is an explosion.

The following are examples of a potential source of hazard.

- In an aircraft a potential source of hazard is an engine
- In a process plant a potential source of hazards is toxic materials

The success of the hazard identification / analysis will depend largely on the model of the system used. This model should genuinely reflect the current system concept / design and should provide sufficient detail on the intended functionality of the system to allow a systematic hazard analysis. A graphical representation of the system can help the hazard identification / analysis team to understand the system. A thorough familiarity shall be acquired of the system, its required control functions and its physical environment. The physical equipment to be included in the scope of the hazard and risk analysis shall be specified. The hazards and hazardous events of the system shall be determined under all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation. Hazards due to interaction with other equipment under control (EUCs) (installed or to be installed) in the proximity of the EUC shall be considered. Information about the determined hazards shall be obtained (toxicity, explosive conditions, corrosiveness, reactivity, flammability etc

Subpractices

- Define, to the greatest extent practicable, the system to be delivered, including the boundary, physical equipment, operating environment and interfaces (physical, functional and logical). Accurately defining the system to be analyzed will enable a more complete set of hazards to be identified. It provides a structured approach to the hazard identification process.
- Determine the high level functions the system is intended to perform. A functional model of the system can provide an effective basis for hazard identification and analysis.
- Use the model of the system as the basis for hazard identification and hazard analysis
- Use a systematic approach that includes consideration of all the phases of the system lifecycle. Systematic approaches include Hazard and Operability Analysis (HAZOP) and Functional Failure Analysis (FFA). Teams of personnel should be formed with consideration given to the effectiveness of those teams. Appropriate personnel should be involved, which may include personnel with:
    - relevant domain experience
    - knowledge of all parts of the system lifecycle (e.g. commissioning, operation, maintenance)
    - experience of hazard identification

Available historical data should be used. This may include information on past incidents/ accidents and checklists specific to the domain.

- Document all hazards identified. Cross reference each hazard to any related analysis.
  Cross reference each hazard to any related safety requirements.
  Cross reference each hazard to any related verification requirements and records.

AP 01.07 Analyze and Prioritize Risks

For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence and determine relative priority.

Description
For safety: For each hazard, determine associated hardware, software, human, and environmental causal factors. For each hazard, determine all potential consequences, including accidents, and assess their severity and likelihood. Severity and likelihood should be combined to obtain an estimate of risk presented by each hazard. Prioritize hazards to apply appropriate resources. In order to avoid obscuring important hazards with insignificant detail, rules are developed to prioritize and select accident sequences for consideration.

For security: Assess the capability and motivation of each threat agent for threats arising from man-made sources. Assess the likelihood of an occurrence for threat events. Gather data related to the properties of the vulnerabilities. Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities. Identify and characterize the unwanted impacts of unwanted incidents with either multiple metrics or consolidated metrics as appropriate. Assess the risk associated with the occurrence of an exposure. Evaluate threat/vulnerability/impact triples (exposures). Assess the total uncertainty associated with the risk for the exposure. Assess risks and determine the probability of occurrence and consequence of realization. Risks are prioritized by likelihood and impact to the organization's information systems.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 13 Risk Management BP 13.02 Identify project risks by examining objectives, alternatives, and constraints in the context of established sources of risk. BP 13.03 Assess risks to determine their likelihood of occurrence and the consequences if they occur.	*Risk Management (RSKM)* RSKM SP 2.1-1 Identify and document the risks. RSKM SP 2.2-1 Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority.

Typical work Products

- Failure Modes and Effects Analysis reports
- Failure Modes Effects and Criticality Analysis reports
- Event Tree Analysis reports
- Fault Tree Analysis reports
- Risk Assessment report
- Risk Indices
- Risk Hazard Index
- Threat Analysis Report
- Safety Criteria Report

- System Threat Analysis Report
- Threat Log
- Benefits-cost Analysis
- Causal Factors List

Notes
For Safety: Determine the conditions and sequences of events that lead to hazards. Systematic causal analysis approaches include Fault Tree Analysis and Event Tree Analysis. The type of accident-initiating events that should be considered, include: system, subsystem or component failure or malfunction (Hardware and Software), environmental conditions; design inadequacies; procedural deficiencies/faults, human/personnel error, dependent failure mechanisms which can cause accident sequences to occur. Document causal factors, ensuring traceability is maintained between the causal factors, hazards and accidents.
Systematic consequence analysis approaches include Failure Modes and Effects Analysis. Severity may be assessed qualitatively (e.g. catastrophic, major, minor) or quantitatively (e.g. 10 fatalities, 1 fatality, 1 severe injury). Likelihood may be assessed qualitatively (e.g. frequent, rare, extremely rare) or quantitatively (e.g. 1 occurrence in 10 years, 1 occurrence every 10,000 operations, 1 occurrence every 100 missions). A quantitative measure of the likelihood of a potential accident is based on the analysis of the hazards for which that accident is a possible consequence. The likelihood of each individual event and co-effector in the event sequence that results in an accident may be drawn from sources such as: manufacturer’s specifications of involved equipment or historical data from previous accidents.
Where systematic failures are seen as contributing to the likelihood of an accident, e.g., where software failures may cause the accident, quantitative analysis is generally seen as inappropriate. Instead, the process is often reversed to set safety targets for system failure rates. Different standards use different terms, such as Safety Integrity Levels, Claim Limits or Levels of Trust, for this concept of assigning qualitative indicators to the required level of protection against systematic failures. In all cases, varying levels of methods, techniques, rules and standards should be associated with the different levels of required protection.

AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan

For each risk associated with safety or security, determine, implement and monitor the risk mitigation plan to achieve an acceptable level of risk.

Description:
For Safety: If the risk does not meet the pre-determined acceptability criteria (refer AP 01.10), an attempt should always be made to reduce it to a level which is acceptable, or if this is not possible, to a level as low as reasonably practicable. The identification of the appropriate risk mitigation measures requires a good understanding of the hazard and the factors contributing to its occurrence, since any mechanism, which will be effective in reducing risk, will have to modify one or more of these factors.

For security: A listing of recommended controls that could mitigate or eliminate the identified risks shall be created. The feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The objective is to select the most appropriate control option or counter measure for minimizing risk. Identify cost-effective controls and determine the most cost-effective control(s) for reducing risk. The purpose of a security assurance strategy is to plan for and ensure that the security objectives are implemented and enforced correctly.

Implement the selected control(s). Note that the implemented controls may lower the risk level but not eliminate the risk. Implement the risk-mitigation activities. Risk-mitigation activities may address lowering the probability that the risk will occur or lowering the extent of the damage the risk causes when it does occur. For risks that are of particular concern, several risk-mitigation activities may be initiated at the same time. Monitor risk-mitigation activities to ensure that the desired results are being obtained.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 13 Risk Management BP 13.04 Develop risk mitigation plans for risks that meet risk action criteria defined by the risk management approach. BP 13.05 Implement, monitor, and control risk mitigation activities in accordance with risk mitigation plans.	*Risk Management (RSKM)* RSKM SP 3.1-1 Develop a risk mitigation plan for the most important risks to the project, as defined by the risk management strategy. RSKM SP 3.2-1 Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.

Typical work products

- Probability Targets
- Threat log
- Risk Mitigation Strategy
- Recommended Safety Requirements
- Risk Mitigation Plan

- Mitigation Strategy

Notes
For safety: Compare risk presented by each hazard with the criteria for acceptability. Some standards do not require the development of risk indices as a combination of likelihood and severity, but use other measures. An example of an alternative measure that is applied in analyzing risk is the level of control that the system has over the initiation or prevention of the hazard.

For risks that exceed the acceptability criteria, determine and document the risk reduction target required to achieve an acceptable level of risk.

Risk mitigation measures may work through reducing the probability of occurrence, or the severity of the consequences, or both. Achieving the desired level of risk reduction may require the implementation of more than one mitigation measure. The possible approaches to risk mitigation include:

- revision of the system design;
- modification of operational procedures;
- changes to staffing arrangements; and
- training of personnel to deal with the hazard.

The earlier in the system life cycle that hazards are identified, the easier it is to change the system design if necessary. As the system nears implementation, changing the design becomes more difficult and costly. This could reduce the available mitigation options for those hazards which are not identified until a late stage of the project.

The effectiveness of any proposed risk mitigation measures must be assessed by first examining closely whether the implementation of the mitigation measures might introduce any new hazards, then evaluating the acceptability of the risk with the proposed mitigation measures in place.

Essential mitigation measures which are necessary for the system to meet the safety assessment criteria are often referred to as *safety requirements*. Implementation of the system cannot proceed until all these safety requirements are met.

Once the system is implemented, particular attention should be paid, when evaluating the results of safety performance monitoring, to verifying that the mitigation measures are working as intended.

For security: Evidence produced through the implementation of a security assurance strategy should provide an acceptable (to the system signature authority) level of confidence that the system security measures are adequate to manage the security risk. Ensure risk reduction strategy includes countermeasures.

AP 01.09 Identify Regulatory Requirements, Laws and Standards

Identify and document applicable regulatory requirements, laws, standards, policies, and acceptable levels of safety and security.

Description
For safety: Applicable regulatory requirements, legal requirements and standards may either be directly applicable to the domain, e.g. avionics, or tailored to the domain. Where such requirements are directly applicable to the domain, they are integrated with requirements that are developed as a result of hazard and risk assessment on the project. Establish and maintain safety criteria that reflect the level of acceptable safety. Select, define, and document the techniques, (measures,) rules, standards and tools required to address safety integrity during each phase of the system lifecycle. Apply the predetermined safety principles (and measures) during each phase of the system lifecycle. Use appropriate techniques and methods depending on the required integrity level.

For security: Management will write a policy stating its need and commitment for information security, and it clearly addresses what types of security are needed, e.g., it addresses what needs to be protected. Management clearly addresses what requirements are needed in the Information Security Policy Document. Identify applicable laws, policies, and constraints. Gather all external influences that affect the security of the system. Select the methods, techniques, and criteria by which system security vulnerabilities in a defined environment are identified and characterized.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 02 Requirements BP 02.02 Identify requirements and constraints pertaining to processes used in providing the required product or service, and pertaining to the context or intended operational environment. *PA 00 Integrated Enterprise Management* BP 00.07 Address the impacts on society of planned activities, products, services, and operations, considering regulatory and legal requirements and risks associated with products, services, and operations.	*Requirements Development (RD)* NEW RD PRACTICE PROPOSED: RD SP 3.25-1 Determine applicable standards: Determine regulatory and legal requirements, policies, and standards that will be applied to the product and its development, manufacturing, operation and support processes.

When implementing BP 02.02 note that nonfunctional requirements and constraints may include regulations, laws, mandates, standards, organizational policy, or principles that are required to be applied in developing or providing a product or service at any or all phases of the life cycle. Identifying constraints pertaining to following certain practices or standards, for example, is part of this practice. A new CMMI practice to address this topic is proposed, as indicated above.

Typical Work Products

- Regulatory requirements
- Legal requirements
- Standards
- Safety principles
- Security principles
- Coding standards
- Design rules and techniques appropriate to each integrity level
- Methods, techniques, and criteria for identifying vulnerabilities
- Application standards
- Order of precedence
- Qualitative or quantitative hazard and risk analysis techniques
- Orders and Policy
- Technical requirements

Notes
For safety:
Safety standards must be applied consistently within a project. In general it is preferable to use the framework of a single safety standard. If multiple safety standards are used, consideration needs to be given to the compatibility of the standards.

Some countries place a legal obligation on suppliers of safety-related equipment or services irrespective of contractual requirements (or lack thereof).

It is a generally accepted concept that absolute safety is unachievable in some situations. In this light, the concept of "acceptably safe" is applied through the definition of what is considered to be an acceptable level of risk. The acceptable level of risk may be defined qualitatively or quantitatively. Levels are usually derived from policies set by government, regulatory bodies, customers or internally within the organization. Criteria may involve target levels for accidents that are classified as catastrophic or critical, or target levels for fatalities caused by the system.

The types of harm that may be considered may include:

- harm to people (fatalities and/or injuries),
- damage to the environment, and
- loss of functionality.

The scope of the hazard and risk assessment should be recorded, to ensure that hazard identification and risk assessment is complete and to provide a record of the justification of any exclusions from the scope.

The criteria for acceptability may be apportioned in various ways. For example, criteria may be based upon the harm attributable to all systems, each system, each subsystem, each accident, or each hazard.

The appropriateness of the techniques, and the extent to which the techniques will need to be applied, will depend on a number of factors, including: the specific hazards and the

consequences; the application sector and its accepted good practices; the legal and safety regulatory requirements; the EUC risk; the availability of accurate data upon which the hazard and risk analysis is to be based. Techniques may include: qualitative or quantitative hazard and risk analysis techniques, Order of Precedence, Precepts, Application standards as tailored .
Use appropriate techniques and methods (project management, documentation, formal methods depending on integrity level)

The design documentation should contain the failure probability target, Safety Integrity Level and corresponding design rules and techniques, and a cross reference to the hazards associated with the function and the relevant risk reduction measures.

AP 01.10 Establish Safety and Security Requirements and Design

Establish and maintain safety and security requirements, including integrity levels, and design the product or service to meet them.

Description
For safety: Safety functional requirements are developed where the hazard identification, hazard analysis and risk assessment has identified hazards that are either unacceptable or are to be reduced. Safety requirements are developed which specify the safety functions that address the hazards and specify the required safety integrity for each safety function. The specification for the safety functions and the specification for the safety integrity together constitute the specification for the overall safety requirements. Typically the requirements specify means of avoiding, mitigating, detecting or reducing the exposure time of the hazard.

Each functional safety requirement should include the level of system integrity required, which describes the level of design, development and test rigor to be applied.

Analyze safety requirements to ensure they are adequately specified and allocate the safety requirements to components. When changes are proposed to the system, such as requirements, design or operational context, an impact analysis is performed to determine impact on safety.

For security: Identify the needs related to security for the system. Collect all information necessary for a comprehensive understanding of customer/stakeholder security needs. Identify how the system's context impacts security. This involves understanding the purpose of the system (for example intelligence, financial, medical). Identify what security objectives should be met to provide adequate security for the system in its operational environment. Define a consistent set of requirements which define the protection to be implemented in the system. Obtain concurrence between all applicable parties on the security requirements. Identify assurance objectives as determined by the customer and identify the level of confidence needed in the system. Develop a high-level security oriented view of the enterprise, including roles, responsibilities, information flow, assets, resources, personnel protection, and physical protection. Coordinate security requirement: work with designers, developers, and users to ensure that all parties have common understanding of security input need.

The low-level design of a TOE provides a description of the internal workings of the TSF in terms of modules and their interrelationships and dependencies. The low-level design provides assurance that the TSF subsystems have been correctly and effectively refined. Identify a solution to security related engineering problem- the purpose of this is to identify alternative solutions to security related engineering problems.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 01 Needs BP 01.01 Identify customers and stakeholders BP 01.02 Elicit customer and other stakeholders' needs, expectations, and measures of effectiveness. BP 01.03 Analyze needs and expectations in the context of the intended operational environment. BP 01.05 Communicate and interact with customers and other stakeholders throughout the life cycle to assure a common understanding of the status and disposition of needs, expectations, and measures of effectiveness. *PA 02 Requirements* BP 02.01 Identify functional and performance requirements, and required product or service attributes, including any requirements pertaining to safety, security, human factors, or other specialized areas. BP 02.02 Identify requirements and constraints pertaining to processes used in providing the required product or service, and pertaining to the context or intended operational environment. BP 02.06 Analyze requirements to ensure that they satisfy established quality criteria including unambiguity, completeness, traceability, feasibility, and verifiability. BP 02.08 Analyze all requirements change requests for impact on the product or service and, upon approval, incorporate the approved changes into the requirements baseline. *PA 03 Design* BP 03.01 Establish and use a mechanism to capture, prioritize, and resolve product and service design issues. BP 03.02 Evaluate alternatives against established criteria to select the architecture, structure, and elements for the product or service design. BP 03.03 Develop interface specifications for the selected product and service elements. BP 03.04 Allocate product and derived requirements to the design elements and interfaces, and to personnel or processes where appropriate. BP 03.05 Define the dynamic interactions and operational sequences among design elements. BP 03.06 Establish design specifications for each element of the product or service. BP 03.07 Establish and use a strategy for managing issues relating to the use of non-developmental item (NDI) product and service elements. BP 03.08 Establish and maintain a complete description of the product and service design.	*Requirements Development (RD)* RD SP 1.1-1. Identify and collect stakeholder needs, expectations, constraints, and interfaces for all phases of the product life cycle. RD SP 1.1-2. Elicit stakeholder needs, expectations, constraints, and interfaces for all phases of the product life cycle. RD SP 3.1-1. Establish and maintain operational concepts and associated scenarios. RD SP 3.2-1. Establish and maintain a definition of required functionality. **NEW RD PRACTICE PROPOSED:** RD SP 3.25-1 Determine applicable standards: Determine regulatory and legal requirements, policies, and standards that will be applied to the product and its development, manufacturing, operation and support processes. *Requirements Management (RM)* RM SP 1.1-1 Develop an understanding with the requirements providers on the meaning of the requirements. RM SP 1.3-1 Manage changes to the requirements as they evolve during the project. *Technical Solution (TS)* TS SP 1.1-1 Develop alternative solutions and selection criteria. TS SP 1.1-2 Develop detailed alternative solutions and selection criteria. TS SP 1.2-2 Evolve the operational concept, scenarios, and environments to describe the conditions, operating modes, and operating states specific to each product component. TS SP 1.3-1 Select the product-component solutions that best satisfy the criteria established. TS SP 2.1-1 Develop a design for the product or product component. TS SP 2.2-3 Establish and maintain a technical data package. TS SP 2.3-1 Establish and maintain the solution for product-component interfaces. TS SP 2.3-3 Design comprehensive product-component interfaces in terms of established and maintained criteria. TS SP 2.4-3 Evaluate whether the product components should be developed, purchased, or reused based on established criteria.

Typical Work Products

- Safety Requirements Specification
- System Requirements Specification (with safety annotations)
- Hazard Log
- Safety Program Plan
- Safety Targets
- System Integrity Levels (SILs)
- Safety Case
- Criteria for design methods
- Design methods
- Design tools
- Technical data package that addresses safety
- System Architecture Document
- Integrated Security Plan

Notes

For safety: For the avoidance of mistakes during the specification of safety requirements, an appropriate group of techniques and measures shall be used. Safety targets may be specified qualitatively or quantitatively. Quantitative targets may be expressed as a frequency of hazardous failure. Qualitative targets may be expressed as an integrity level. A qualitative target may be derived as a result of a quantitative target where the qualitative target is intended to satisfy the quantitative target, but generally does not guarantee satisfaction of that quantitative target.

Where systems suffer from systematic failures, e.g., software systems, quantitative targets are often replaced by qualitative targets. System Integrity Levels (SILs) are sometimes used to translate the required reliability of a safety function to the processes used to develop and test that safety function. Such translations are not reversible.

All safety requirements should be traceable to the respective hazard(s) and the causal factor(s) that it is mitigating. Sometime more than one requirement is developed to mitigate a causal factor.

NOTE: The specification of the safety integrity requirements is an interim stage towards the determination of the safety integrity levels for the safety functions to be implemented by the safety-related systems. Some of the qualitative methods used to determine the safety integrity levels progress directly from the risk parameters to the safety integrity levels. In such cases the necessary risk reduction is implicitly rather than explicitly stated because it is incorporated in the method itself.

The safety requirements shall be expressed and structured in such a way that they are: a) clear, precise, unequivocal, unambiguous, verifiable, testable, maintainable and feasible; and b) written to aid comprehension by those who are likely to utilize the information at any stage of the safety lifecycle.

The requirements developed shall be formally reviewed by the organizations concerned, and agreement reached.

Subpractices

- Determine any hazards associated with each functional safety requirement. This can be achieved through derivation from the risk assessment of each hazard
- Review the acceptability of the hazards associated with each safety function and the associated risk reduction target. This can be achieved through derivation of the risk reduction targets that was set for each hazard during hazard analysis and risk assessment.
- Set a safety integrity target for each functional safety requirement commensurate with the risk reduction target.
    - The safety integrity target should ensure the level of risk presented by the system will be less than or equal to the acceptable risk, and should ensure the estimates of assessed risk used in the hazard analysis and risk assessment are carried forward into the system design. For software intensive systems and complex electrical or electronic systems, this is usually specified as an integrity level.
    - It may be infeasible to determine if a safety integrity target has been met, e.g., where failures are systematic in nature or where failure rates are sufficiently low to make testing prohibitively time consuming. In such cases, safety integrity targets may be used in determining how the product is to be developed, and such translations from quantitative goals to qualitative methods are generally not used in reverse.
- Ensure that each functional safety requirement has an associated safety integrity target or safety integrity requirement.
- Use appropriate design methods and techniques to design the safety-related product Refer to AP 01.02 and AP 01.09 for further information on the selection and application of appropriate design methods and techniques.
- Allocate safety requirements to components.

Safety requirements are allocated to components in a manner consistent with the capabilities of the components

- Analyze product and service needs
- Requirements need to address threats and threat risk reduction strategies
- Discuss integrity levels and what they are

New hazards, review outcomes and deviations from plans should initiate corrective action.
All changes to undergo safety impact analysis.
All modification which have an impact on safety shall initiate a return to the appropriate phase of the safety lifecycle, and all subsequent phases shall be repeated for the change.
Modifications shall apply the same level of rigor as that applied for the original system.

AP 01.11 Objectively Evaluate Products

Objectively verify and validate the work products and delivered products and services to assure safety and security requirements have been achieved and products and services fulfill intended use.

Description
For safety: Evaluate safety work products throughout the system lifecycle to assure the level of risk associated with a system (residual risk) has been reduced to a tolerable level. This activity usually involves more than traditional Verification and Validation activities. An *independent* evaluation of the safety program, associated work products and residual risk is performed to arrive at a determination of the level and acceptability of safety achieved. The safety program, work environment and associated work products are assessed to demonstrate compliance with the regulatory, legal and contractual requirements (e.g. tailored standards) and the safety principles. It shall also be determined if the proposed risk reduction techniques (such as architectural design, test coverage, design rigor, procedures, training etc) are sufficient to achieve the hazard probability/risk reduction targets. This can be achieved through techniques such as Fault Tree Analysis for the random element, and auditing to ensure that the appropriate design rules and techniques are being implemented for the systematic element. Formal analyses may also be employed to determine if hazard probability targets can be met.

For security: Ensure solutions are verified and validates with respect to security. Identify the solution to be verified and validated. Define the approach and level of rigor for verifying and validating each solution. Verify that the solution implements the requirements associated with the previous level of abstraction. Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs. Capture the verification and validation results for the other engineering groups. The information security policy will have an owner who is responsible for its maintenance and review according to a defined review process. Perform analysis of security assurance evidence. Review adequacy of the risk assessment and obtain a decision to proceed, modify, or cancel the effort based on risks.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 08 Evaluation BP 08.01 Establish and maintain a comprehensive strategy and requirements for evaluating products and services throughout their life cycle. BP 08.02 Develop the detailed procedures, methods, and processes to be used in evaluating products and services. BP 08.03 Establish and maintain the tools, facilities, personnel, documentation, and environment needed to perform planned evaluations. BP 08.04 Evaluate incremental work products and	*Verification (VER)* VER SP 1.1-1 Select the work products to be verified and the verification methods that will be used for each. VER SP 1.2-2 Establish and maintain the environment needed to support verification. VER SP 1.3-3 Establish and maintain verification procedures and criteria for the selected work products. VER SP 2.1-1 Prepare for peer reviews of selected work products. VER SP 2.2-1 Conduct peer reviews on selected work products and identify issues resulting from the peer

iCMM Implementing Practices	*CMMI Implementing Practices*
services. BP 08.05 Evaluate end-products and services against specified requirements. BP 08.06 Evaluate the capability of end-products and services to fulfill their intended use in representative operational environments. BP 08.07 Analyze results of evaluations and compare them to the needs and requirements to identify and quantify deficiencies, and recommend corrective and preventive actions.	review. VER SP 2.3-2 Analyze data about preparation, conduct, and results of the peer reviews. VER SP 3.1-1 Perform verification on the selected work products. VER SP 3.2-2 Analyze the results of all verification activities and identify corrective action. *Validation (VAL)* VAL SP 1.1-1 Select products and product components to be validated and the validation methods that will be used for each. VAL SP 1.2-2 Establish and maintain the environment needed to support validation. VAL SP 1.3-3 Establish and maintain procedures and criteria for validation. VAL SP 2.1-1 Perform validation on the selected products and product components. VAL SP 2.2-1 Analyze the results of the validation activities and identify issues.

Ensure objectivity is addressed and assurance argument requirements are addressed when performing implementing practices.

Typical Work Products

- Safety Assessment Plan
- Safety Assessment Report
- Security Assessment Report
- Safety Case
- Safety Evaluation Report
- Independent Assessment Report
- Compliance Assessment Report
- Security Test and Evaluation Plan
- Security Test and Evaluation Report
- Independent Verification and Validation Test

Notes

For safety: Produce recommendations for Acceptance, Qualified Acceptance or Rejection. Appropriate levels of independence and competence shall be maintained, according to the safety integrity level. Some standards specify levels of independence to achieve sufficient objectivity. Independence is important for ensuring that:

- Evaluators are not put under unreasonable pressure to acquiesce on safety issues, and
- Evaluators consider the design from a fresh perspective and reveal problems that might not be spotted by those who are closer to the design.

Documents, analyses, products, product components (e.g. code, operating procedures), work products (e.g. coding standards), tools (development, support) etc. are included for evaluation. Refer to AP01.02 for further information on what is included in the work environment. Ensure adequate verification of safety requirements and features and adequate validation of system safety (inc. assumptions, procedures etc). Provide a comprehensive evaluation of the functional safety achieved and the residual safety risk.

An independent evaluation is carried out by investigating the project and the products/system developed by the project. The evaluation includes:

- familiarization with the system/product,
- familiarization with the hazards of the system/product, and
- review and analysis of project deliverables

The evaluation may also include reworking of parts of the safety work carried out by the project. Typically the evaluator presents findings and recommendations to the person/body responsible for safety acceptance. The recommendations of the evaluator are used as part of the final decision of the acceptance body.

Depending on the integrity level, safety evaluations (or safety assessments) may include:

- Architectural analysis
- Fault Tree Analysis
- Failure Analysis,
- Checklists,
- Decision/Truth Tables,
- Software Complexity Metrics,
- Common cause failure analysis of diverse software
- Reliability block diagram
- Reliability models
- Formal Proof
- Probabilistic Testing
- Static Analysis
- Dynamic Analysis and Testing
- Diagnostic Coverage

Sub-Practices:

- Plan for Safety Assessment
- Ensure personnel are appropriately trained and qualified to undertake assessment activities.
    - Minimum competence levels
    - Assessment of competence
- Conduct Safety Assessment

For security: Assurance evidence analysis is conducted to provide confidence that the evidence that is collected meets the security objectives, thus satisfying the customer's security needs.

AP 01.12 Establish Safety and Security Assurance Argument

Establish and maintain safety and security assurance arguments and supporting evidence throughout the lifecycle.

Description

An assurance argument is a set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied.

For safety:
Establish and maintain a Hazard Record. The status of hazards provides a good basis for monitoring and controlling project progress against safety matters. Once a hazard has been identified and documented, it should be tracked to closure. Establish and maintain a safety argument and supporting evidence throughout the system lifecycle. A safety case or safety assessment report presents an argument for the safety of the product / system being developed by the project.

For security: An overall assurance argument is developed to demonstrate compliance with security assurance objectives and provided to the customer.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 08 Evaluation BP 08.07 Analyze results of evaluations and compare them to the needs and requirements to identify and quantify deficiencies, and recommend corrective and preventive actions. *PA 15 Quality Assurance and Management* BP 15.04 Record and report the results of quality assurance activities to applicable stakeholders.	*Verification (VER)* VER SP 3.2-2 Analyze the results of all verification activities and identify corrective action. *Validation (VAL)* VAL SP 2.2-1 Analyze the results of the validation activities and identify issues. Process and Product Quality Assurance (PPQA) PPQA SP 2.2-1 Establish and maintain records of the quality assurance activities.

Typical Work Products

- Threat Record
- Threat Log
- Threat status summaries
- Action requests
- High level safety argument
- Cross references to supporting evidence
- Safety Case
- Safety Analysis Report

Notes

For Safety:
To effectively track a hazard to closure, the status of each hazard must be monitored regularly. Example hazard information to be logged is:

- A complete description of the hazard
- Who identified the hazard and when
- What are the consequences of the hazard and the severity of any resulting accidents
- What could cause the hazard
- Risk assessment of the hazard
- Causal Factors
- How the hazard will be detected, controlled or mitigated
- Safety requirements that are derived from the hazard
- Where the safety requirements are addressed in the design
- Verification requirements that are derived from the safety requirements
- Verification records
- Cross-references to other documents (that may document the above).

A safety case should consist of two parts – the main part which provides a coherent argument for the safety of the product, and a set of supporting evidence. It can be advantageous to release the safety case in stages through the project, in order to gain early acceptance of the project safety approach. Also, for some products it is helpful to produce multiple documents that make up the overall safety case, in which case the structure of the documents should be clear.

Not all safety standards require the development of a safety case. In such cases, other documents may be used to achieve the same goal.

The safety argument should be clear, consistent, complete, comprehensible (to all stakeholders) and defensible and should cover all stages of the system lifecycle. In order to ensure the argument is readable, supporting evidence is cross-referenced from the main body of the argument. Examples of safety case content include:

- a high level summary of the safety argument
- relevant standards and regulatory requirements
- the configuration baseline
- all identified hazards; and the residual risk of each hazard
- all operational and support assumptions
- all safety related design decisions and features, along with the rational for these decisions and features

Typically the supporting evidence will be the safety documentation that has been developed throughout the project safety lifecycle and will include plans, specification, analysis reports, verification reports and validation reports. Examples of supporting evidence to a safety case are:

- evidence of hazard identification and risk assessment activities
- evidence of system hazard analysis activities
- evidence of all safety assurance activities, including the results of safety assessments

AP 01.13 Establish Independent Safety and Security Reporting

Establish and maintain independent reporting of safety and security status and issues.

Description

For safety: Establish and maintain a safety organization structure, including specifying roles and duties of personnel and groups, providing reporting channels, and ensuring adequate levels of managerial and technical independence. Both an enterprise and project safety organization structure should give consideration to the need for managerial and technical independence in the conduct of safety-related activities. It should also make provision for the resolution of disputes relating to safety.

The organizational requirements needed to support the core safety management functions must address:

- responsibility and accountability;
- the need for and the role of a safety manager;
- training and competency of personnel; and
- safety documentation.

For security: A security infrastructure is created so information security can be managed within an organization. A forum of management is created to promote security through out an organization once a information security policy is created. Security is coordinated over all parts of an organization. Representatives from each part meet with management to implement information security. Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined. Responsibilities should be defined in the Information Security Policy. Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

Implementing practices:

This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 00 Integrated Enterprise Management BP 00.01 Establish, maintain, and communicate a strategic vision that identifies long-term goals, values, performance expectations, and core activities. BP 00.02 Align the enterprise to operate efficiently and consistently to achieve the vision. *PA 11 Project Management* BP 11.08 Identify individuals or teams that will be assigned the resources and responsibilities for meeting project objectives. *PA 15 Quality Assurance and Management* BP 15.04 Record and report the results of quality assurance activities to applicable stakeholders.	*Organizational Environment for Integration (OEI)* OEI SP1.1 Establish and maintain a shared vision for the organization. *Integrated Project Management (IPM)* IPM SP 4.1-1 Determine the integrated team structure that will best meet the project objectives and constraints. *Process and Product Quality Assurance (PPQA)* PPQA SP 2.1-1 Communicate quality issues and ensure resolution of noncompliance issues with the staff and managers.

Typical Work Products

- Project Organization Chart
- Enterprise level organization chart
- Policy
- Safety Manual
- Safety Work Plan
- Periodic Reviews
- Issue Tracking System

Notes

For safety:

- Responsibility and accountability are closely related concepts. Each individual member of staff has a responsibility for his or her actions.
- Safety must be supported from the very top of the organization and must be seen as an integrated strategic aspect of the overall business management, to ensure that safety is given the necessary priority by the organization.
- The safety manager should ideally have no responsibilities other than safety. This would generally be the case in large organizations where a full time safety manager position can be justified. In smaller organizations, safety management may have to be the responsibility of a manager who also has other duties. It would be preferable, in such cases, that the person responsible for safety management did not also have direct responsibility for any of the operational or engineering areas, to avoid possible conflicts of interest.
- Having staff who are competent for the job they are performing is a fundamental prerequisite for achieving safety. Competency requirements, and where appropriate licensing requirements, should be documented in the job description for each safety-related position. These requirements should then be reflected in the recruitment requirements and internal training course content for these positions.
- It is also important that the organization be able to provide evidence of the measures taken to control risks, and ensure that adequate levels of safety are maintained. The safety management system should therefore incorporate provisions to ensure that all safety-related decisions and actions are adequately documented. Records should be maintained of all:
  - safety occurrence and investigation reports;
  - safety audit reports;
  - periodic analyses of safety trends; and
  - safety assessment documentation.

Independence is important for ensuring that:

- staff in a safety role are not put under unreasonable pressure to acquiesce on safety issues, and
- staff who are responsible for independent verification, validation or assessment consider designs from a fresh perspective and reveal problems that might not be spotted by those who are closer to the design.

Example roles to be documented in a project safety organization structure:

- acceptance body
- certification body
- safety management group
- (system) safety working group/committee
- safety manager
- safety engineers
- safety authority
- quality assurance

For security:

- Identify how security will coordinated over an organization
- Communicate and document security decisions and recommendations among the various security engineers, other engineering groups, information systems security personnel, external entities, and other appropriate parties.
- Define specific processes to support effective interaction with customer(s) and supplier(s).
- Establish and maintain an integrated management plan that defines project interaction with all internal and external organizations (e.g., the subcontractor) performing the technical effort.
- Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined.
- Responsibilities must be defined in the information security plan.

AP 01.14 Establish a Safety and Security Assurance Plan

Establish and maintain a plan to achieve safety and security assurance requirements and objectives.

Description
For safety: Establish and maintain a safety plan to achieve overall safety requirements and objectives through out the lifecycle.

For security: The security implementation plan prioritizes the implementation actions and projects the start and target completion dates. This plan will aid and expedite the risk mitigation process. Identify resources that are critical to the technical success of the project. Ensure a bottom-up, common understanding of the process, resources, schedule, and information requirements by affected groups and individuals throughout the project. Inputs on the project plan are solicited from all responsible organizational elements and project staff. Develop a project plan. Obtain commitment to the plan.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 00 Integrated Enterprise Management BP 00.04 Establish, integrate, and deploy tactical action plans to accomplish strategic objectives. *PA 11 Project Management* BP 11.01 Define project objectives, scope, and the work products and services that are to be provided by the project. BP 11.06 Establish and maintain a complete set of plans for providing the products and services throughout the project life cycle. *PA 13 Risk Management* BP 13.01 Establish and maintain an approach for managing risk that is the basis for identifying, assessing, mitigating, and monitoring risks for the life of the project.	*Organizational Innovation and Deployment (OID)* OID 2.1-1 Establish and maintain the plans for deploying the selected process and technology improvements. *Quantitative Project Management (QPM)* QPM SP 1.1-1 Establish and maintain the project's quality and process-performance objectives. *Project Planning (PP)* PP SP 2.7-1 Establish and maintain the overall project plan content. *Risk Management (RSKM)* RSKM SP 1.3-1 Establish and maintain the strategy to be used for risk management.

Typical Work Products

- Safety Strategy
- Safety Plan
- Safety verification plan
- Safety validation plan
- Independent safety assessment plan
- Safety Acceptance Plan
- Skills and experience matrix

- Safety Training plan
- Security Training Plan
- Security Plan

Notes:
For safety:
The safety plan defines a program that is planned, integrated, and developed in conjunction with other design, development, production, and quality control functions. The planning should cover safety engineering and support processes for safety verification, validation and independent safety assessment activities, such as audits and evaluations. The safety program plan should be adapted to suit the type of system and reflect the activities to be carried out during each phase. Plan for the management of safety during the operation, maintenance and disposal of the product. Many standards specify particular methods and techniques that are considered to be suitable for safety-related work. The methods and techniques may vary according to the complexity and/or integrity level of the products being developed. These issues should be considered in safety planning.

A safety plan generally addresses:

- selection of safety lifecycle
- identification of safety work products to be developed
- specify safety measurement goals and objectives
- integration of safety analysis with system development
- identify risk assessment procedures, hazard analysis techniques
- hazard tracking and resolution procedures, including mitigation, review and acceptance procedures
- reference to detailed description of the process of deriving safety requirements and the rules and techniques for each LOT or SIL.
- verification techniques
- schedules for system safety review evaluation activities

Document a safety lifecycle for the project and system. The project safety lifecycle should be integrated into the overall project lifecycle. The system safety lifecycle should cover all system phases, from initial concept through to disposal including quality and assurance procedures. Safety needs to be ensured throughout the lifecycle. In particular, safety issues should be addressed as early as possible.

Safety acceptance of the project plans and the product should be sought at key points in the project lifecycle. In order to ensure the risk of major acceptance problems arising late in the project is reduced, projects should aim to obtain staged acceptance as the project progresses. The planning should document the key stages of the acceptance, what will be delivered for assessment and who will provide acceptance at each stage.

For safety-related activities it is particularly important that staff have adequate experience, training and skills. In certain domains this can also include licensing schemes that ensure staff are licensed before they undertake unsupervised safety-critical work. Planning should address competency requirements in terms of expected qualifications, skills, and years of experience, training requirements where there are shortfalls against the competency requirements, and recruitment requirements where it is not possible to training existing staff to the required competency. Establish internal reporting and corrective action system and procedures for disposition of mishaps/incidents and test failures. Manufactures should maintain a system to initiate changes to allow users to readily check whether the system has been subject to a safety recall.

For security: A project plan is established and maintained as the basis for managing the project

- Estimate scope of the project
- Define project life cycle
- Determine estimates of cost, schedule
- Plan Project resource and needed knowledge/skill
- Plan stakeholder involvement
- Identify project risk
- Reconcile work and resource level
- Obtain Plan commitment

AP 01.15 Select and Manage Suppliers, Products and Services

Select and manage products and suppliers using safety and security criteria.

Description:
For safety: Analyze the project's needs to acquire safety-related products and services, and select suppliers. Establish supplier agreements that include safety requirements. Execute supplier agreements that include safety requirements and ensure that safety assurance is delivered with the product or service. Supplier agreements are executed and monitored.

For security: Establish security requirements. Maintain the security of information when the responsibility for information processing has been outsourced to another organization. Acquire COTS products. Execute supplier agreements. Conduct verification and validation.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 05 Outsourcing BP 05.01 Identify needed solution or process components that may be provided by other/outside organizations. BP 05.02 Identify suppliers that have shown expertise or capability in the identified areas. BP 05.03 Prepare for the solicitation/tasking and the selection of a supplier, including objective review of estimates of cost for the services/products to be outsourced, a clear description of tasking, and inclusion of evaluation criteria in the solicitation/tasking package. BP 05.04 Choose suppliers in accordance with the selection strategy and criteria. BP 05.05 Establish and maintain communication with suppliers emphasizing the needs, expectations, and measures of effectiveness held by the acquirer for the solution or process components that are being acquired.	*Supplier Agreement Management (SAM)* SAM SP 1.1-1 Determine the type of acquisition for each product or product component to be acquired. SAM SP 1.2-1 Select suppliers based on an evaluation of their ability to meet the specified requirements and established criteria. SAM SP 1.3-1 Establish and maintain formal agreements with the supplier. SAM SP 2.1-1 Review candidate COTS products to ensure they satisfy the specified requirements that are covered under a supplier agreement. SAM SP 2.2-1 Perform activities with the supplier as specified in the supplier agreement. SAM SP 2.3-1 Ensure that the supplier agreement is satisfied before accepting the acquired product. SAM SP 2.4-1 Transition the acquired products from the supplier to the project.
PA 12 Supplier Agreement Management BP 12.01 Ensure the supplier adheres to acquirer-approved planning documents. BP 12.02 Review and monitor supplier activities through periodic, formal reviews and informal, technical issue interchanges with the supplier, and by quantitative means to continuously determine agreement outcomes versus plans and requirements. BP 12.03 Ensure agreements comply with current laws, policies and regulations, and incorporate necessary and approved changes into the agreement. BP 12.04 Monitor supplier's quality assurance, configuration management, test, corrective action and risk management systems, plans and process activities,	*Integrated Supplier Management (ISM)* ISM SP 1.1-1 Identify and analyze potential sources of products that may be used to satisfy the project's requirements. ISM SP 1.2-1 Use a formal evaluation process to determine which sources of custom-made and off-the-shelf products to use. ISM SP 2.1-1 Monitor and analyze selected processes used by the supplier. ISM SP 2.2-1 For custom-made products, evaluate selected supplier work products. ISM SP 2.3-1 Revise the supplier agreement or relationship, as appropriate, to reflect changes in conditions.

iCMM Implementing Practices	*CMMI Implementing Practices*
results, and products. BP 12.05 Perform activities to foster a partnership between the acquiring organization and the supplier. BP 12.06 Analyze and direct the performance of agreement activities. BP 12.07 Ensure the agreement is being maintained and followed, and all changes and records are properly processed, controlled and maintained. BP 12.08 Determine whether to accept the supplier's product or service, based on acceptance conditions stipulated in the agreement. *PA 09 Deployment, Transition, and Disposal* BP 09.05 Transfer the product or service to the customer/stakeholder operation and support organizations**.**	

Typical Work Products

- Supplier agreements that include safety requirements
- Supplier management plan
- Subcontract management plan
- Safety Requirements Specifications
- System Requirements Specifications (with safety/security annotations)
- Review minutes
- Audit records
- Security Requirements Specification

Notes

For safety: Ensure that all products and services that will be acquired are assessed to establish whether or not they are safety-related. In general, the project should assume that all products and services that will be acquired are safety-related unless it is proven otherwise. Care should be taken to select an appropriate supplier. Suppliers should be assessed to ensure they have appropriate processes, skills and experience for supplying safety-related products and services.

Establish an agreement that includes relevant safety requirements. The agreement should cover the following:

- how the supplier will interact with the project on safety matters (e.g. lines of communication for safety matters, which link into the project safety organization structure)
- the commitment of both the project and the supplier to participate in the ongoing safety activities (e.g. through participation in a safety working group)
- the need to deliver a safety case as part of the safety-related product or service. Allowance for the monitoring activities that are necessary.

Procedures should be in place to monitor progress and performance of safety-related suppliers e.g. through regular progress reviews and/or audits examining safety-related activities. Supporting the supplier may involve the inclusion of the organization in meetings of groups within the supplier such as the System Safety Working Group.

The project should ensure that suitable safety assurance is delivered with any product delivered as part of the agreement (e.g. in the form of a safety case).

Establish traceability between the organization and the supplier. In general, the majority of safety requirements flow from the organization to the supplier. Assumptions made by either party may need to be propagated throughout the system to check their validity. Safety analysis of the supplier may need to be constructed and used in the context of wider safety analysis of the organization. Other issues requiring traceability include schedules, competencies, and other support practices.

Special consideration should be given where Commercial Off The Shelf (COTS) products are acquired. Example considerations that are important when acquiring COTS products are:

- Transfer of existing safety assurance of the COTS product into a suitable form for the project
- The operational history of the COTS product
- Ensuring compatibility with the original environment of an COTS product when transferring assurance or using operational histories
- Accurate identification of the configuration or version of COTS products
- Ensuring any transferred assurance or operational history applies to the version of the COTS product supplied
- Identifying and analyzing unspecified functionality of COTS products
- Ongoing support of the COTS product

AP 01.16 Monitor and Control Activities and Products

Measure, monitor and review safety and security activities against plans, control products, take corrective action, and improve processes.

Description
For safety: Review the project's progress relative to the safety program both periodically and at selected milestones throughout the system lifecycle.
Ensure safety is continuously maintained and managed throughout the entire system lifecycle. The safety management system should incorporate provisions to ensure that all safety-related decisions and actions are adequately documented and controlled. Records should be maintained of all. Copies of all safety related documentation must be retained for a period equivalent to the lifecycle of the system or change (and processed according to current organizational guidelines). The effort put into safety performance monitoring and investigation will only produce dividends, in the form of improved safety performance, if the lessons learned from the investigation and analysis of all the data are taken on board by the organization, and translated into actions. The action required can range from changes at the organizational level, to procedures or structure, through to changes in individual patterns of behavior.

For security: Monitor project against plan. Manage corrective action to closure. The Information Security Policy should be reviewed independently to provide assurance that organizational practices properly reflect the policy. Manage the response to security relevant incidents. The capabilities of the CM system address the likelihood that accidental or unauthorized modifications of the configuration items will occur. The CM system should ensure the integrity of the TOE from the early design stages through all subsequent maintenance efforts.
The objective of this family is to ensure that all necessary TOE configuration items are tracked by the CM system. This helps to ensure that the integrity of these configuration items is protected through the capabilities of the CM system.

Implementing practices:
This application practice is implemented by performing the following practices, in the safety and security assurance context.

iCMM Implementing Practices	*CMMI Implementing Practices*
PA 16 Configuration Management BP 16.01 Establish roles, responsibilities, and methods for the application of CM activities. BP 16.02 Identify configuration items, interim work products, and work environment items that will be baselined or placed under version control, and baseline them. BP 16.03 Establish and maintain a repository to house work product baselines. BP 16.04 Control changes to baselined work products through tracking, recording, review, and approval processes throughout the life cycle. BP 16.05 Record and report change information about	*Configuration Management (CM)* CM SP 1.1-1 Identify the configuration items, components, and related work products that will be placed under configuration management. CM SP 1.2-1 Establish and maintain a configuration management and change management system for controlling work products. CM SP 1.3-1 Create or release baselines for internal use and for delivery to the customer. CM SP 2.1-1 Track change requests for the configuration items. CM SP 2.2-1 Control changes to the configuration items.

iCMM Implementing Practices	*CMMI Implementing Practices*
the baselined configuration items. BP 16.06 Conduct configuration audits and inspections to verify integrity of the baselines and check the work products for compliance with the baselines. ***PA 15 Quality Assurance and Management*** BP 15.01 Establish, document, imp1ement, and maintain a quality management system. BP 15.02 Objectively monitor compliance of performed activities with the established processes throughout the life cycle. BP 15.03 Objectively measure work products and services against the requirements and standards that define them. BP 15.04 Record and report the results of quality assurance activities to applicable stakeholders. BP 15.05 Analyze quality records and measurements to detect the need for corrective action and develop recommendations for quality improvement or corrective and preventive actions. BP 15.06 Initiate activities that address identified quality issues or quality improvement opportunities. BP 15.07 Evaluate the effect of changes after they have been implemented. *PA 00 Integrated Enterprise Management* BP 00.05 Review performance relative to goals and changing needs across the enterprise. BP 00.06 Translate performance review findings into action. *PA 11 Project Management* BP 11.10 Monitor and track project activities and results against plans. BP 11.11 Conduct formal and informal reviews of project performance and analyze variances from plans. BP 11.12 Take corrective actions to address problems. *PA 18 Measurement and Analysis* BP 18.01 Establish measurable objectives from issues and goals and identify the specific measures that will provide the basis for performance analysis. BP 18.02 Collect and verify measurement data and generate results. BP 18.03 Store measurement data and results in a repository. BP 18.04 Analyze data to determine performance against goals. BP 18.05 Report results of measurement and analysis to all affected stakeholders. *PA 21 Process Improvement* BP 21.01 Identify process improvement goals from the organization's business goals.	CM SP 3.1-1 Establish and maintain records describing configuration items. CM SP 3.2-1 Perform configuration audits to maintain integrity of the configuration baselines. *Process and Product Quality Assurance (PPQA)* PPQA SP 1.1-1 Objectively evaluate the designated performed processes against the applicable process descriptions, standards, and procedures. PPQA SP 1.2-1 Objectively evaluate the designated work products and services against the applicable process descriptions, standards, and procedures. PPQA SP 2.1-1 Communicate quality issues and ensure resolution of noncompliance issues with the staff and managers. PPQA SP 2.2-1 Establish and maintain records of the quality assurance activities. *Organizational Innovation and Deployment (OID)* OID 2.2-1 Manage the deployment of the selected process and technology improvements. OID 2.3-1 Measure the effects of the deployed process and technology improvements. *Project Monitoring and Control (PMC)* PMC SP 1.1-1 Monitor the actual values of the project planning parameters against the project plan. PMC SP 1.2-1 Monitor commitments against those identified in the project plan. PMC SP 1.3-1 Monitor risks against those identified in the project plan. PMC SP 1.4-1 Monitor the management of project data against the project plan. PMC SP 1.5-1 Monitor stakeholder involvement against the project plan. PMC SP 1.6-1 Periodically review the project's progress, performance, and issues. PMC SP 1.7-1 Review the accomplishments and results of the project at selected project milestones. PMC SP 2.1-1 Collect and analyze the issues and determine the corrective actions necessary to address the issues. PMC SP 2.2-1 Take corrective action on identified issues. PMC SP 2.3-1 Manage corrective actions to closure. *Measurement and Analysis (MA)* MA SP 1.1-1 Establish and maintain measurement objectives that are derived from identified information needs and objectives. MA SP 1.2-1 Specify measures to address the measurement objectives. MA SP 1.3-1 Specify how measurement data will be obtained and stored.

iCMM Implementing Practices	*CMMI Implementing Practices*
BP 21.02 Plan improvements to the project/organization's processes based on widespread participation and analysis of the impact of potential improvements on achieving the goals of the organization. BP 21.03 Appraise the processes periodically. BP 21.04 Analyze appraisal results and other sources for improvement and establish an action plan for process improvement. BP 21.05 Implement the process improvement action plan. BP 21.06 Confirm that improvement activities meet goals and desired results. BP 21.07 Sustain and deploy improvement gains across all applicable parts of the organization/project. BP 21.08 Continuously monitor and improve process performance.	MA SP 1.4-1 Specify how measurement data will be analyzed and reported. MA SP 2.1-1 Obtain specified measurement data. MA SP 2.2-1 Analyze and interpret measurement data. MA SP 2.3-1 Manage and store measurement data, measurement specifications, and analysis results. MA SP 2.4-1 Report results of measurement and analysis activities to all relevant stakeholders. *Organizational Process Focus (OPF)* OPF SP 1.1-1 Establish and maintain the description of the process needs and objectives for the organization. OPF SP 1.2-1 Appraise the processes of the organization periodically and as needed to maintain an understanding of their strengths and weaknesses. OPF SP 1.3-1 Identify improvements to the organization's processes and process assets. OPF SP 2.1-1 Establish and maintain process action plans to address improvements to the organization's processes and process assets. OPF SP 2.2-1 Implement process action plans across the organization. OPF SP 2.3-1 Deploy organizational process assets across the organization. OPF SP 2.4-1 Incorporate process-related work products, measures, and improvement information derived from planning and performing the process into the organizational process assets.

Typical work products

- Operational error deviation report
- Safety trend report
- Hazard Tracking System
- Safety Library
- Lessons Learned

Notes

For safety: Safety Committee endorses outputs. Document in hazard log.
New hazards, review outcomes and deviations from plans should initiate corrective action.
All changes to undergo safety impact analysis. All modification which have an impact on safety shall initiate a return to the appropriate phase of the safety lifecycle, and all subsequent phases shall be repeated for the change. Modifications shall apply the same level of rigor as that applied for the original system. All information with safety implications should be disseminated widely, and should be clear, concise and easy to read. Information can be disseminated by means of formal reports to management, and by safety newsletters, bulletins and seminars for all staff. However, the lessons associated with a particular occurrence will not really have been learned until action is taken to reduce the probability of similar occurrences in the future. Management must therefore ensure that, where necessary, procedures are modified, and the lessons learned are reflected in relevant training courses. Safety data that could be of interest to

other organizations or States should be shared as widely as possible. States should promote the establishment of safety information sharing mechanisms among all users of the aviation system in order to facilitate the free exchange of information on actual and potential safety deficiencies.

For security: Monitor compliance. Monitor project risks. Conduct progress/milestone review. Monitor project-planning parameters. Manage corrective action to closure. Analyze issues. Take corrective action. Manage corrective actions.

Term or Phrase	Definition	Source
Assurance Argument	A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied	SSE-CMM
Assurance Claim	An assertion or supporting assertion that a system meets a safety or security need. Claims address both direct threats (e.g., system data are protected from attacks by outsiders) and indirect threats (e.g., system code has minimal flaws)	Adapted from SSE-CMM
Causal Factor	Root cause. An act, omission, condition, or circumstance that either starts or sustains an accident sequence or a security compromise. A causal factor may be related to hardware, software, human, and/or the environment. A given act, omission, condition, or circumstance is a causal factor if correcting, eliminating, or avoiding it would prevent the accident or security compromise or mitigate damage or injury	Adapted from United States Department of Agriculture - Thirty Mile Fire Investigation
Common cause failure	Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure	IEC 61508
Dependent failure	Failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it	IEC 61508
Diagnostic coverage	Fractional decrease in the probability of dangerous hardware failure resulting from the operation of the automatic diagnostic tests	IEC 61508
Fault	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function	IEC 61508
Functional safety assessment	Investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities	IEC 61508
Hazard	Potential source of harm	IEC 61508
Hazard probability	The aggregate probability of occurrence of the individual events that create a specific hazard	MIL-STD-882C
Integrity	Freedom from flaw or corruption	Synthesized by the Safety and Security Assurance project from multiple sources
Integrity Level	A denotation of a range of values of a property of an item necessary to maintain system risks within tolerable limits. For items that perform mitigating functions, the property is the	ISO 15026

Term or Phrase	Definition	Source
	reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure.	
Reliability	The property of consistent behavior and results (e.g., mean time between failure)	SSE-CMM and IEEE 13335-1:1996
Residual risk	Risk remaining after protective measures have been taken	IEC 61508
Risk	(1) A condition (relating to the development or operation of a product or service) that has been recognized as having the possibility of resulting in loss, harm, or other adverse consequences (2) an estimate of the probability of occurrence and the severity of consequences if the loss, harm or other adverse consequences occur	Synthesis of definitions of risk from: IEC 61508, DEF-STAN-0056, MIL-STD-882C, NIST 800-30, SSE-CMM, and others
Risk Assessment (security)	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact Part of Risk Management and synonymous with Risk Analysis.	NIST 800-30
Safety	Freedom from unacceptable risk	IEC 61508
Safety integrity	Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time	IEC 61508
Safety integrity level	An indicator of the required level of safety integrity	DEF-STAN-0056
Safety target	A numerical expression of the policy on the tolerability of risks from a system, giving for each identified accident its highest tolerable probability for each group of people who may be harmed by it	DEF-STAN-0056
Security	The combination of confidentiality, integrity and availability that is intended to protect products, services , and people from harm	Synthesized from NIST 800-30 and other sources
Security Policy	Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems	SSE-CMM
Signature Authority	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk	SSE-CMM
System safety	The characteristic of a product or service that indicates freedom from harm or potential harm	Synthesized from MIL-STD-

Term or Phrase	Definition	Source
		882C and other sources
Systematic failure	Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors	IEC 61508
Threat	An entity with potential to cause harm to an organization, person, product or service (includes persons, organizations, governments, and environmental phenomena such as storms)	Synthesized by the Safety and Security Assurance project from multiple sources
Threat Analysis	The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.	NIST 800-30
Vulnerabilit y	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.	NIST 800-30

Note:

(1) Definitions are from the sources that were used to develop the Application Area, where available

(2) Terms that are in the iCMM or CMMI are not included